

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
17 July 2003 (17.07.2003)

PCT

(10) International Publication Number  
**WO 03/058408 A2**

- (51) International Patent Classification<sup>7</sup>: **G06F 1/00**
- (21) International Application Number: **PCT/DK03/00016**
- (22) International Filing Date: 10 January 2003 (10.01.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
PA 2002 00036 10 January 2002 (10.01.2002) DK
- (71) Applicant (for all designated States except US): **NEUPART APS** [DK/DK]; Vesterbrogade 149, DK-1620 Copenhagen V (DK).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **NEUPART, Lars** [DK/DK]; Gammel Kongevej 174, DK-1850 Frederiksberg C (DK).
- (74) Agent: **NIELSEN, Henrik, Sten**; Budde, Schou & Ostensfeld A/S, Vester Søgade 10, DK-1601 Copenhagen V (DK).
- (81) Designated States (national): AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**  
— without international search report and to be republished upon receipt of that report
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: **INFORMATION SECURITY AWARENESS SYSTEM**

(57) Abstract: A computer system for providing security awareness in an organization, comprises: a memory means, an input device, constituted by a hard disk or Random Access Memory device, a central processo unit connected to the memory means, an input device, constituted by a mouse or keyboard device, and an output device, constituted by a printer or display device. The input device is connected to the central processor unit, for the input of a piece of security information into the computer system for storing the security information in the memory means as an information security object. The output device is connected to the central processor unit for the output of security information. The system further comprises a policy module communicating with the input device and the memory means for the conversion of the piece of security information into the information security object to be stored in the memory means, and a survey module communicating with the memory means and the output means for generating from the information security object an element of a questionnaire to be output by means of the output device.

**BEST AVAILABLE COPY**

## Information Security Awareness system

The invention relates to a computer system and a method providing on a modular platform security policy management, security survey, security education, risk analysis and management, incident management and audit functions to individuals in an organization. The elements are used all together or separately. By utilizing the technique according to the invention users gain multilanguage security policies and rules, policy based and auto generated surveys, increased security awareness, increased knowledge and ability to impact their actions in a security cautious way. The organization, e.g. a business enterprise or company, gain lower cost of developing, maintaining and communicating security policies and rules, increased information security, increased return of investment in existing security technologies and products and reduced risk of costly security incidents.

The method is operated in two alternative set-up's: 1) in a hosted environment in order to provide the defined functions and services. 2) Stand-alone execution runs on servers at business users or business partners in order to provide the defined functions and services.

The computer system operates on a standard business style networked computer, for example a server type computer with hard drives, computing power, memory and input/output devices or the system operates on a dedicated computer device with storage capacity, computing power, memory and input/output devices.

The method and the computer system according to the invention is preferably implemented using software running on computers. The software contains user interface modules for each of the modules, business logic, persistence, an information security object database as well as interfaces between the users and the modules and interfaces in between the modules or services.

User interface to modules.

The technique according to the invention provides full functionality to users through an Internet browser, e.g. MS Internet Explorer, Netscape, Mozilla, or Opera.

The Email messages are used to direct users to the appropriate network address accessed by an Internet Browser.

Alternatively, the user interface to the modules is implemented using stand-alone applications (versus browser based).

Security policy applied to common data security architecture, e.g. United States Patent Application 20010018746 which is an architecture allowing users to generate trust policies independent of the computers they have the responsibility of managing.

Security management system and security managing method, e.g. United States Patent Application 20010023486, which is a database based security management and security audit system. This invention is about having users managing systems.

American vendors Pentasafe and Intellitactics' provide security policy management tools or services: One is a product named "Livingpolicy", another is "Vigilant Policy Manager". Both also provide simple surveying functions. Yes/No questionnaires which refer to security policy requirements are known prior to this invention.

Electronically performed surveys with functions which allows a manager type user, e.g. a security manager or e.g. an officer to put in free text style questions in a number of questionnaires to users are known.

E-learning systems and learning management systems are known. Security learning classes, also web based, are known. These classes target system administrators, or network administrators or security administrators, and do not target all relevant users in an organisation.

In some organisations or contexts the terms "security instruction" "security rule", or "security procedure" are used instead or together with of the term "security policy".

The technique according to the present invention is supporting multiple languages both in

terms of the software itself and in terms of the content elements, e.g. the information security.

5 The policy module is a tool for security policy management. The users of the module use the Policy module to generate and manage a set of easy to use security policies. The content in these policies is re-used in the survey module and in the education module.

10 In this context, the term a "policy" is to be understood as a number of records in the policy table in the Information Security Object database (ISO-DB). The records relate to a specific customer organization and contain the following content.

| Object<br>Category<br>and sub<br>category | Object<br>descriptor | Object<br>Content | Content<br>category | Target group |
|---|----------------------|-------------------|---------------------|--------------|
|   |                      |                   |                     |              |

15 The *Customer* is an identifier optionally linking to a separate customer table further optionally linking to a CRM system. The operator (or superuser) creates a customer of the customer table of the database after receiving an order or after agreeing to a demonstration for a specific client.

20 The *Object Category* identifies the type of information security object to which the record relates. It contains text. E.g. does the information security object impact "computer user behavior", does it impact only the "IT-department", or is it about "physical access". There will typically be a number of Information security objects with the same content category. Example: More than one information security object is to regulate the physical access to the customer's information assets.

25 The *Information security object descriptor* is the object description itself; it contains a text string or a link to a text string describing the object. Examples include: "Passwords are required to contain a variety of different character types." and "Passwords are required to have a minimum length". Objects are unique within the customer's policy, and the Manager selects the information security object from lists of object templates which content providers define. These lists are stored in tables

for Information security object templates. Objects which are not already in the policy are marked e.g. "Unused", or "New", or Customer specific".

The *Object Content* holds the content or the value of the Information security object.

- 5 The value is a text string. The Manager chooses the content from a list where all entries relate to the Information security object. Example: If the Information security object specifies that a certain password length is required, the object content field contains the exact value, e.g. "eight characters" and the list contains a number of other content which in some cases are acceptable. In the list, a field named "default security rating" indicates which Object Content options content providers consider
- 10 the more secure choices.

The *Content category* describes to which content categories the ISO belongs. Example: "Passwords", "Computer security", "Network Access".

- 15 The *Target group* describes to whom the ISO relates. the number of ISO's within Security policies tends to become large. The effect of this value is reduction of the number of ISO's presented to individual group of users.

- 20 A superuser adds name of security policy into the information security object database (ISO-DB).
- Either a Default security policy is created:
  - Superuser specifies the "default Security level profile" of the organization.
  - The system queries all information security objects (ISO) which matches the
- 25 default security level profile and adds the result to the information security policy for the organization, hereby generating a default current security policy.

Or, the ISO's are created by ISO's containing existing text format security policies, security instructions, or security procedures.

- 30 The default security policy is subsequent managed by a management user: Information Security Objects are added, edited or deleted.

Those ISO's not included in the current security policy are listed as e.g. unused objects, making it easy for the management user to see, monitor and review these ISO's deliberately not used in the current policy.

5 Unused ISO's are made current by a simple selection.

New ISO's – e.g. organizational-specific objects - are added to customer's current policy by the management user entering the required content, e.g. content category, descriptor and value.

10 New default ISO's are added as the outcome of information security research performed by content providers.

15 The policies (or the security instructions, procedures etc) are published, distributed or communicated to the end users through email, web servers (e.g. Internet, extranet or intranet sites) and not at least through the survey module and the education module.

20 The users of the policy module are by default and unless otherwise defined the same throughout all modules.

- Managers, who will typically be customer's security manager or security officer or consultant or a content provider who provides a manual policy service to the customer.
- Superusers, who may be content providers.
- 25 • Users, who will be computer users in the organizations of the customer.

The following table shows an example of user permissions:

| <b>User group:</b>  | <b>Users</b> | <b>Managers</b> | <b>Superusers</b> |
|---|--------------|-----------------|-------------------|
| <b>Function:</b>  |              |                 |                   |
| Read policy   | ✓            | ✓               | ✓                 |
| Add policy  |              | ✓               | ✓                 |
| Modify policy   |              | ✓               | ✓                 |
| Delete policy   |              | ✓               | ✓                 |
| Read information security objects                             | ✓            | ✓               | ✓                 |
| Add information security objects                              |              | ✓               | ✓                 |
| Modify information security objects                           |              | ✓               | ✓                 |
| Delete information security objects                           |              | ✓               | ✓                 |
| Read object content   | ✓            | ✓               | ✓                 |
| Add object content  |              | ✓               | ✓                 |
| Modify object content   |              | ✓               | ✓                 |
| Delete object content   |              | ✓               | ✓                 |
| Read object content templates                                 |              | ✓               | ✓                 |
| Add custom object content templates                           |              |                 | ✓                 |
| Modify custom content templates                               |              |                 | ✓                 |
| Delete content templates                                      |              |                 | ✓                 |
| Acknowledge policy read and understood                        | ✓            |                 |                   |
| Add Comment to Information security object and object content | ✓            |                 |                   |
| Add, invite and delete users                                  |              | ✓               | ✓                 |
| Add, invite and delete managers                               |              |                 | ✓                 |

|   |   |   |   |
|---|---|---|---|
| Read survey content                       | ✓ | ✓ | ✓ |
| Add custom survey content                 |   | ✓ | ✓ |
| Modify custom content templates           |   | ✓ | ✓ |
| Delete content templates                  |   |   | ✓ |
| Initiate surveys                          |   | ✓ | ✓ |
| Answer surveys                            | ✓ |   |   |
| Read survey reports                       |   | ✓ | ✓ |
| Edit survey reports                       |   |   | ✓ |
| Read and participate in learning sessions | ✓ | ✓ | ✓ |
| Update lessons                            |   | ✓ | ✓ |

Display warning when user is trying to modify information security objects and object values which are already used in policies and have been read by users. Warning should suggest to consider adding a new object and value instead.

5

Information security objects and Object Contents are versioned and time stamped at last modification.

10

For Policy users, yet unread information security objects and object contents are marked "New".

15

The survey module invites users at specified intervals to answer a questionnaire regarding general security knowledge and security policy specific knowledge. Invitations are made on manager's or user's request. Invitation e-mails are sent to users directly from the module to invited users or to customer's administrator. Emails contain a direct link (URL) to an online questionnaire relating to the customer and containing sufficient access information for the user to gain access to the questionnaire. The content of the invitation email is customizable and includes a default content provided.



The authentication of the survey users is based upon user's ability to receive an email at the specified email, by user name and password, or by digital certificates, or by LDAP-protocol to an external system or by other authentication method.

- 5 The user or users is or are presented to a short privacy policy description with a link to a wording which comfortingly and clearly describes what user data are stored and how the results of the survey will be used and by whom.

10 Users choose to respond anonymously resulting in that no personal information is stored, but the answers from the individual user are consolidate in the survey results. This feature provides that the manager chose to allow anonymous answers. Users choosing the anonymous option will be informed that questions might be repeated in later surveys and education.

15 The Survey system logs which users have answered, and a reminder process is initiated for those who did not participate before a deadline specified by the Manager. Default reminder is typically 7 days after first invitation email. Users are associated with a number of group descriptions to enable grouped reporting and to allow targeted, efficient follow up education.

20

Users are provided with their score and the right answers immediately. Administrator receives a report which documents the responses and provides summary to make it easy to identify weak points in security chain and to educate efficiently in the right places.

25

The Survey is repeated periodically as requested by the organization. The repetition allows to document the security level development and to add new components to policy or to awareness program as recommended.

30 The content of the survey questions and the defined right answers comes from a number of question pools. One pool is general knowledge questions and another is automatically derived from the ISO's.

The module generates survey result reports which are easy to read for people without security knowledge in e.g. executive staff or management as well as for security officers and managers. The reports contain graphically presented survey results documenting e.g. the following items:

- 5      • Total knowledge score for company compared to average of all Survey respondents.
- Total knowledge score for company compared to average in same business vertical.
- Historical development in knowledge score with each previous survey results  
10      plotted along a time axis.
- Total knowledge score grouped by department.
- Total knowledge score grouped by Policy Categories.
- Department knowledge score grouped by Object content category.
- Historical development grouped by department.
- 15      The module also generates a report so that individual Users may see their own personal security score development chart.

The module supports PGP encrypted emails to administrator, by allowing administrator to upload public PGP Key.

- 20      The lessons contained in the education module are presented to the users with E-learning lessons in the education module. The lessons are using content from the central security object database.

- 25      The lessons which by default are offered to the user depends on the results from the survey module and upon which ISO content categories the Manager has chosen to activate for the customer organization to which the user belongs.

The user and the Manager have the option to select and de-select other modules

than offered by default.

E-learning lessons or modules exist for each ISO content category and for many types of Information security objects.

5

An e-learning lesson lasts e.g. 20 – 30 minutes to complete for an average user.

The lessons are able to communicate both the generic information security content and content of the security policies in a motivating, appealing and catching way.

10

An audit module pulls out selected ISO's as defined by the policy module or by other modules. An audit list is generated automatically with all or selected ISO's. Each ISO constitutes a potential control point. For each control point it is indicated whether or not compliance is established. It is possible to make notes to the compliance statement. Users of the audit module may be central security officers requiring other parts of an organization to comply with various policies. Alternatively, the users may be employees who do self assessment of their policy compliance. Further alternatively, the users may be internal or external auditors, who are auditing the security policy compliance of an organization.

15

20

A risk analysis module defines, structures and contains the content of risk analysis report. This includes physical and information based assets, vulnerabilities, threats, risk or likelihood of incidents, as well as consequences when/if incidents happen. The Risk Analysis module is linked to ISO's so that ISO's can be selected in order to reduce risk if desired.

25

An incident module defines, structures, logs and contains the content of security incidents. This includes incidents to physical and information based assets. The incident module is linked to ISO's so that ISO's can be selected in order to reduce risk of incident re-occurring if desired. The incident module links to the Risk analysis module so that historical logged data can be used to improve accuracy of risk or likelihood of incidents in the Risk analysis module.

30

The database module contains the core data structures if the system

These structures are implemented on a database platform which

- Can be distributed as full runtime versions to deliver a "in a box" type solutions-.
- 5 • Gives a high level of platform in-dependencies in order to solve high security requirements.

The Management module includes:

- Common user management routines for the three modules
- 10 • User access and authentication modules.
- Data maintenance routines and interfaces.

Admissions are authenticated at a higher level than end users, in order to meet the requirements of easy access to end users and high security in the system.

- 15 Using e-learning systems – online and offline - provides information security lessons with generic content to all - or to groups of - computer users throughout any organisation.

*Effects:* Users gain better understanding of general information security aspects and can operate their work place computer with increased information security as a  
20 result.

Using e-learning systems – online and offline - provides information security lessons with organisation-specific content to all - or to groups of - computer users throughout any organisation.

- 25 *Effects:* Users gain better understanding of the security policies, descriptions, procedures and requirements in the organisation of which they are a member. Users can process and work with organisation's information security assets, e.g. documents, data, general information security aspects in an increased secure way, compared to if users have not obtained this understanding through the invention.

Using multimedia, e.g. sound, speak, voices, animations, moving pictures, video recordings and recorded computer screen shots provide information security learning to computer users throughout the organisation.

*Effects:* Users become increasingly motivated to learn information security and to return to the learning process for further increased learning.

Having general Information security content and questions in electronically performed computer user surveys, the users receive the right security answers together with their own answers.

*Effect:* Survey participants become increasingly aware of the content in the survey. Users learn security. A survey report or management reports can be generated. A survey report can document the information security awareness among the computer users in the organisation. The survey results can also be used to target succeeding education more efficiently. The targeting can be done by groups of the organisation, or by individual.

The information security content is preferably provided as individual (for an organisational) Information security content and questions in electronically performed computer user surveys.

*Effects:* Survey participants become increasingly aware of the organisational-specific content in the survey. A survey report or management reports can be generated. A survey report can document the specific knowledge about the information security awareness among the computer users in the organisation. The survey results can also be used to target succeeding education more efficiently. The targeting can be done by groups of the organisation, or by individual.

The technique according to the invention provides information security awareness, security lessons and security surveys targeted to computer users throughout the organisation.

*Effects:* The weakest link in the information security link is strengthened by the invention. The information security link consists of technology/products/systems as well as end user behaviour. End users without sufficient knowledge are the weakest

link, and when strengthened through the invention, end users can choose a secure behaviour when working and when using computers to process information assets.

5 *Information security policies, Information security procedures, Information security instructions or, Information security rules are saved in a relational database. These document types are modularised and saved in a database as information security objects (ISO's) The objects contain, for example, specific or general information security objects and appropriate content or values of such objects.*

10 *Example: Assume a traditional style security policy specifies user' behaviour to be using password(s) with a certain minimum length, and assume that length is e.g. 6 characters long. In the relational database one record would be added with minimum the following information security object content:*

- 15 *1) Content category is "user behaviour",  
2) descriptor is "passwords with a certain minimum length are required to be used" and  
3) the actual length which is required.  
4) Target groups are "users" who need to set their password and "it-staff" who needs to set computer systems to enforce the minimum length*

20 *Example 2: Assume a traditional style security policy stipulates rules for how users shall treat information assets. On area of regulations is about employees having papers and documents on the desktops. Users are required to clean their desktop for confidential papers by the end of each working day. In the relational database one record would be added with minimum the following information security object content:*

- 25 *1) Content category is "information asset handling",  
2) "rules for cleaning employees desktop for information, e.g. documents and papers"  
3) Employees must clean their desktop by the end of each working day.  
30 4) The target group is "office employees of Company XYZ, Inc."*

*Effect: Database based security policies, security procedures, security instructions, or security rules can be created, managed and be in other contexts with less manual efforts compared to traditional security policies and traditional policy management*

tools. The increased effectiveness also has the effect of increased information security to organizations and to users as security policies, security procedures, security instructions, or security rules are foundations for improved information security in organizations of any type.

5

The ISO's are stored in a database and are used as modular content for e.g. Information security policies, Information security procedures, Information security instructions, and Information security rules. The ISO's are assigned an unique identifier allowing organizations which create and maintain e.g. security policies to link to the identifier. The ISO's are also assigned values for "default security level value". The ISO's are also assigned a status value for each organization.

10

*Effects:* Increased re-use of ISO's, as organizations can choose and select content without "re-writing" default ISO's to go into their policies.

15

By specifying a default security level value for a specific organisation, the invention makes it possible to automatically create a default policy, simply by querying the default ISO's which match the default security level value of the organisation.

The status value for each ISO makes it possible for a management user of an organisation to define values which sets the status. For example, ISO's with value "new since last" or "ready for review" can be processed and can be assigned a new status e.g. "Current" meaning it now is a part of the current policy. Similarly the status values can also have the effect of identifying which ISO's deliberately are not included in a policy, e.g. with the value "Unused". The status value also makes it possible to add custom content in an organisation's policies, since e.g. the value "Custom" can be used as such.

20

25

The content of the information security objects are utilised for automatically generating relevant content of information security surveys. The ISO's which are also content in security policies are utilised for surveying e.g. user conformance, understanding, knowledge and awareness of the defined and current security policies and of information security aspects more general.

30

*Effects:* The surveys are generated much more effortlessly by re-using ISO's than by using traditional survey content and preparation methods.

The surveys contain more accurate and relevant content for the user.

Organizations using this invention gain more accurate reporting on topics of relevance and improved information security.

5

### Example Content in survey

The organisational specific parts of the survey are queried in the information security object database.

| <b>Question</b>   | <b>Answer options</b>  | <b>Right Answer</b>  | <b>Comment</b>                              |
|---|--|--|---|
| Does your company have a set of security policies?  | Yes/No   | As defined in ISO-DB   |   |
| How aware are you about the content of the policies?  | Fully/well/some/not at all   | Not defined  |   |
| According to your knowledge, does your company have policies or rules about "<Object Category>"           | Yes/No/Don't know  | Yes if <Policy Category> is found in current policy                                    | Repeat until all categories have been asked |
| According to your knowledge, does your company have a policy which defines <Information security object>" | Yes/No/Don't know  | Yes if <Information security object> is found in current policy                        | Repeat until all objects have been asked    |
| According to your knowledge, what does the policy say about <information security object>"                | List all Object Content Templates for the Information security object. | The Object Content which is defined in the Policy for this Information security object | Repeat until all objects have been asked    |



For the general security knowledge part of Survey, the questions, answer options and right answers are managed by the Manager and Superuser in a way similar to the Policy Management.

A survey consists of a link to a policy, a number of questions, answer options, and indication of the right answer option together with a score for each option. Default score for the right answer is 10 and default score for wrong answers is 0.

Questions are stored in a table in the security object database.

The answers are stored in a table which links to the user, to the questions and to the survey. If user requested to be anonymous, the answers are added to answer consolidation tables which allow for the Result reports to be generated without saving individual user responses.

The ISO's are used as (part of) the content in security learning.

Effects: Users of the information learning system will be presented not only with general knowledge, but also with the specific content of the organisation they belong to.

Users will learn not only the general knowledge but will also learn what ISO's manager users have decided are relevant for the users to know in their organization.

The ISO's are used as (part of) the content in audit reports. Audit reports link to specific security policies.

*Effects: Internal or external auditors can audit specific security policy compliance.*

*Audit reports reflecting real security policies and their control points can be generated with less manual work efforts. The invention can auto generate control points based upon ISO's.*

Content from the ISO's are linked with contents in risk analysis reports (RAR).

*Effects: RAR's can identify risk areas and ISO's in security policies can be used to reduce those risks, if desired by the organization and/or the users. Policies made with this link become more targeted to reduce real risks than without the link.*

The incident module is linked to ISO's. The incident module links to the Risk analysis module.

*Effects: ISO's in security policies can be selected more efficiently and can reduce risk of incident re-occurring if desired. Historical logged data can be used to improve accuract of risk or likelihood of incidents in the Risk analysis module.*

5 The user settings and permissions which are defined in the management module are re-used in the policy, survey and the education modules.

Effects: Users can without the need for repeating authentication routines (e.g. passwords) be educated and surveyed in e.g. security policies, security instructions, security surveys, security learning.

10

In the accompanying drawings, a first and presently preferred embodiment of the computer system according to the present invention is shown.

15 In Fig. 1, a diagramatic view is shown illustrating the structure of the computer system and the software thereof comprising centrally an information security object database ISO-DB connected through respective interfaces designated interface A, interface B, interface C and interface D to a policy module, a survey module, an educational module and a management module, respectively. The modules are further connected through respective interfaces to the users, either directly or  
20 through a network to the user PC's.

25 In Fig. 2, a route diagram is shown illustrating the security policy creation technique according to the present invention. It is contemplated that the diagram and the text thereof is self-explanatory and therefore, no detailed description of the diagram is presented.

30 In Fig. 3, a block diagramatic view of the security policy management method and a system according to the present invention is shown. The block diagramatic view is contemplated to be self-explanatory and therefore, no detailed description of the diagram is presented.

Although the present invention has been described with reference to specific applications and a specific embodiment, the present invention is also to be

contemplated including any modification obvious to a person having ordinary skill in the art and therefore, the scope of the invention is to be considered in view of the apending claims.

**PATENT CLAIMS**

1. A computer system for providing security awareness in an organization, comprising:

5                   a memory means, constituted by a hard disk or Random Access Memory device,

                  a central processor unit connected to said memory means,

                  an input device, constituted by a mouse or keyboard device, connected to said central processor unit, for the input of a piece of security information into said  
10 computer system for storing said security information in said memory means as an information security object,

                  an output device, constituted by a printer or display device, connected to said central processor unit for the output of security information,

                  a policy module communicating with said input device and said memory  
15 means for the conversion of said piece of security information into said information security object to be stored in said memory means, and

                  a survey module communicating with said memory means and said output means for generating from said information security object an element of a questionnaire to be output by means of said output device.

20 2. The computer system according to claim 1, further comprising an educational module communicating with said memory means for receiving through said input device a set of answers to said questionnaire and for comparing said set of answers of said questionnaire with said information security objects for determining the  
25 correct and the incorrect answers, and generating, based on said incorrect answers, an educational program to be output by means of said output device.

3. The computer system according to claim 2, said set of answers being stored in said memory means.

30 4. The computer system according to any of the claims 1-3, said memory means being organized as a database.

5. The computer system according to any of the claims 1-4, said computer system constituting a stand alone computer or alternatively a computer system including a network and a plurality of PC's each including an input device and an output device to be operated by a respective user.

5

6. The computer system according to any of the claims 1-5, said central processor unit controls in said conversion of said piece of said security information into said information security object, said policy module to check in said memory means the possible presence of a corresponding security information object.

10

7. A method of providing security awareness in an organization, comprising the steps of providing a piece of security information, storing said piece of security information in a memory means as an information security object, said information security object being generated in a policy module, generating in a survey module an element of a questionnaire from said information security object and output said questionnaire including said element.

15

8. The method according to claim 7, further comprising any of the features of the computer system according to any of the claims 1-6.

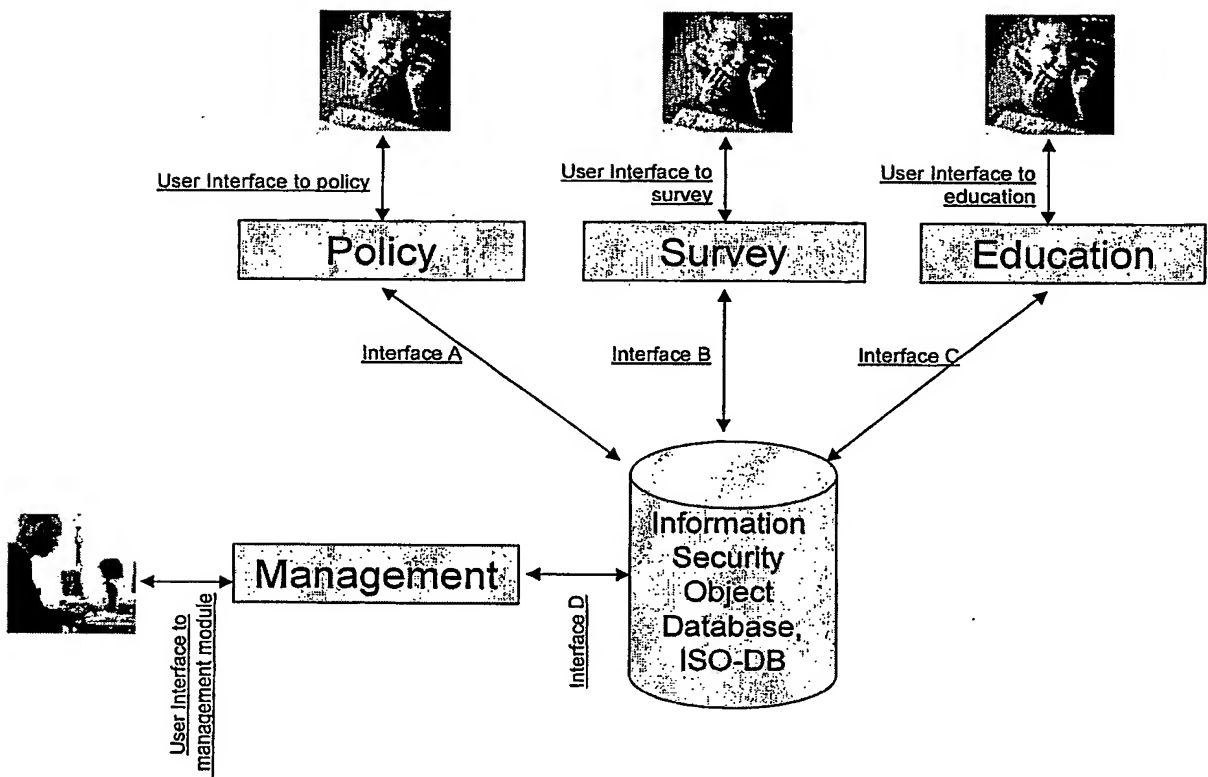


Fig. 1

## Security Policy Creation

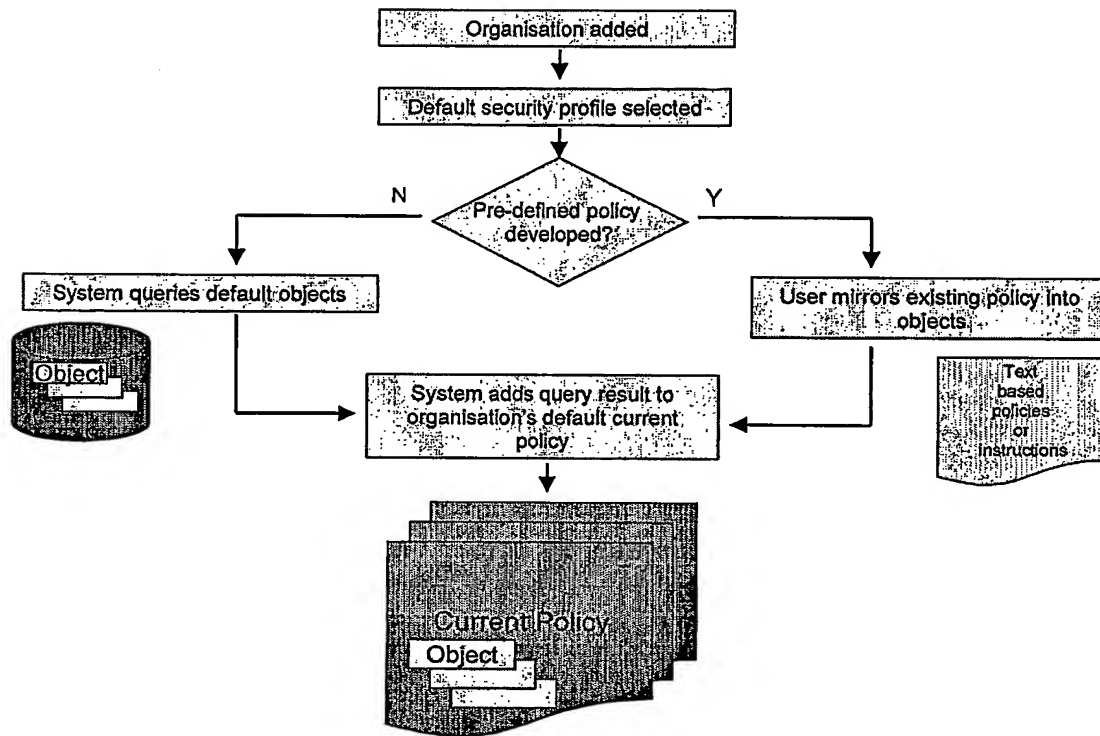


Fig. 2

## Security Policy Management

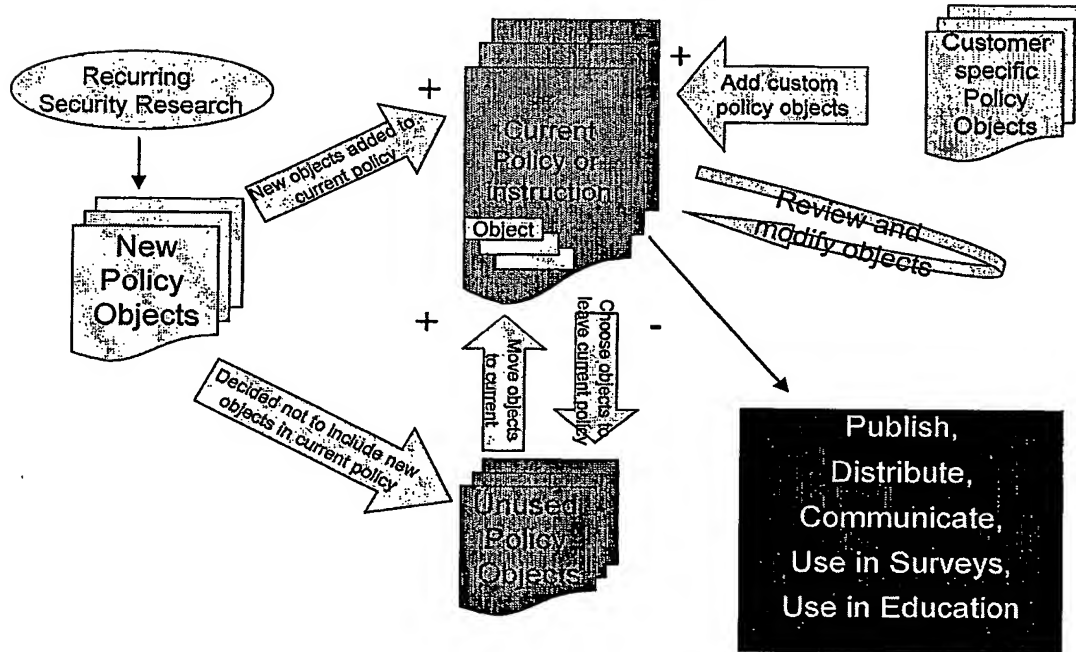


Fig. 3



(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
17 July 2003 (17.07.2003)

PCT

(10) International Publication Number  
**WO 03/058408 A3**

(51) International Patent Classification<sup>7</sup>: **G06F 1/00**, 17/60

(21) International Application Number: PCT/DK03/00016

(22) International Filing Date: 10 January 2003 (10.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
PA 2002 00036 10 January 2002 (10.01.2002) DK

(71) Applicant (for all designated States except US): NEUPART APS [DK/DK]; Vesterbrogade 149, DK-1620 Copenhagen V (DK).

(72) Inventor; and

(75) Inventor/Applicant (for US only): NEUPART, Lars [DK/DK]; Gammel Kongevej 174, DK-1850 Frederiksberg C (DK).

(74) Agent: NIELSEN, Henrik, Sten; Budde, Schou & Ostfeld A/S, Vester Søgade 10, DK-1601 Copenhagen V (DK).

(81) Designated States (national): AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA,

CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

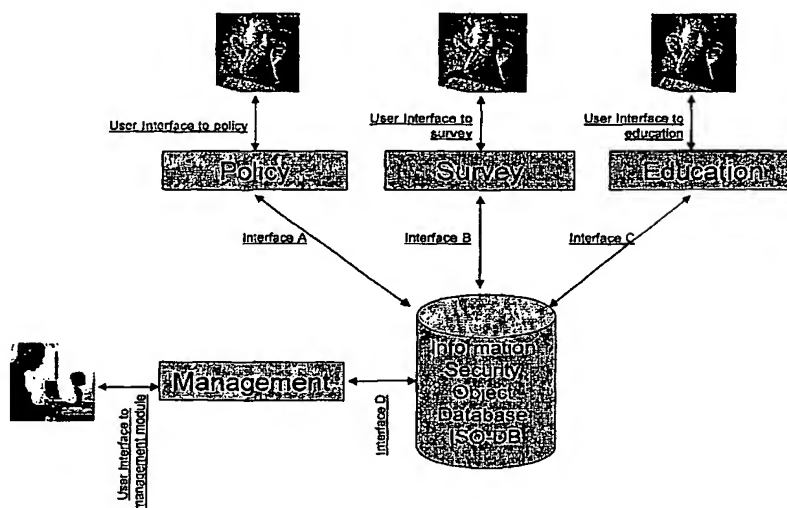
Published:

— with international search report

(88) Date of publication of the international search report:  
18 December 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: INFORMATION SECURITY AWARENESS SYSTEM



(57) Abstract: A computer system for providing security awareness in an organization, comprises: a memory means, an input device, constituted by a hard disk or Random Access Memory device, a central processor unit connected to the memory means, an input device, constituted by a mouse or keyboard device, and an output device, constituted by a printer or display device. The input device is connected to the central processor unit, for the input of a piece of security information into the computer system for storing the security information in the memory means as an information security object. The output device is connected to the central processor unit for the output of security information. The system further comprises a policy module communicating with the input device and the memory means for the conversion of the piece of security information into the information security object to be stored in the memory means, and a survey module communicating with the memory means and the output means for generating from the information security object an element of a questionnaire to be output by means of the output device.

WO 03/058408 A3

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP03/00016

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EP0-Internal, WPI Data, PAJ

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
|------------|---|-----------------------|
| X          | EP 1 160 645 A (ASGENT INC)<br>5 December 2001 (2001-12-05)<br>column 2, line 33 -column 17, line 57<br>abstract; claims 1,8-11,17-19; figures<br>2,4,8-11<br>--- | 1-8                   |
| X          | EP 1 160 643 A (ASGENT INC)<br>5 December 2001 (2001-12-05)<br>column 2, line 32 -column 11, line 15<br>abstract; claims 1-5; figures 2,4<br>---                  | 1-8                   |
| A          | WO 99 67931 A (JACOBSON FAMILY HOLDINGS<br>LLC) 29 December 1999 (1999-12-29)<br>page 2, line 22 -page 3, line 15<br>abstract<br>---<br>-/--                      | 1-8                   |

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

12 May 2003

Date of mailing of the international search report

20. 06. 2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

PÄR HEIMDAL/JA A

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 03/00016

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
|------------|---|-----------------------|
| A          | EP 0 999 489 A (CITIBANK NA)<br>10 May 2000 (2000-05-10)<br>column 2, line 15 -column 4, line 29<br>abstract  | 1-8                   |
| P,X        | ---<br>US 2002/188861 A1 (TOWNSEND TIMOTHY J)<br>12 December 2002 (2002-12-12)<br>paragraph [0010]<br>paragraph [0024]<br>abstract; figure 2                        | 1-8                   |
| E          | ---<br>US 2003/065942 A1 (WIERSCHEM SCOTT R ET<br>AL) 3 April 2003 (2003-04-03)<br>paragraph [0008] - paragraph [0009]<br>abstract; claims 1,4,8; figure 2<br>----- | 1-8                   |

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/DK 03/00016

| Patent document<br>cited in search report |    | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|---|----|---------------------|----------------------------|---------------------|
| EP 1160645                                | A  | 05-12-2001          | JP 2002056176 A            | 20-02-2002          |
|   |    |                     | EP 1160643 A2              | 05-12-2001          |
|   |    |                     | EP 1160645 A2              | 05-12-2001          |
|   |    |                     | US 2001049793 A1           | 06-12-2001          |
| -----                                     |    |                     |                            |                     |
| EP 1160643                                | A  | 05-12-2001          | EP 1160643 A2              | 05-12-2001          |
|   |    |                     | EP 1160645 A2              | 05-12-2001          |
|   |    |                     | JP 2002056176 A            | 20-02-2002          |
|   |    |                     | US 2001049793 A1           | 06-12-2001          |
| -----                                     |    |                     |                            |                     |
| WO 9967931                                | A  | 29-12-1999          | AU 4703899 A               | 10-01-2000          |
|   |    |                     | EP 1090492 A1              | 11-04-2001          |
|   |    |                     | WO 9967931 A1              | 29-12-1999          |
| -----                                     |    |                     |                            |                     |
| EP 0999489                                | A  | 10-05-2000          | EP 0999489 A2              | 10-05-2000          |
| -----                                     |    |                     |                            |                     |
| US 2002188861                             | A1 | 12-12-2002          | US 6374358 B1              | 16-04-2002          |
|   |    |                     | AT 233918 T                | 15-03-2003          |
|   |    |                     | AU 5896999 A               | 28-02-2000          |
|   |    |                     | DE 69905726 D1             | 10-04-2003          |
|   |    |                     | EP 1101159 A1              | 23-05-2001          |
|   |    |                     | WO 0008543 A1              | 17-02-2000          |
| -----                                     |    |                     |                            |                     |
| US 2003065942                             | A1 | 03-04-2003          | NONE                       |                     |
| -----                                     |    |                     |                            |                     |

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ ~~FADED~~ TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ ~~SKewed~~/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**